Exam : C1000-082

Title : IBM Spectrum Protect V8.1.9 Administration

https://www.passcert.com/C1000-082.html

1.What is indicated when a security notification is displayed in the Operations Center?
A. a possible ransomware attack
B. a restricted command has been issued and needs approval
C. an SSL/TLS failure
D. too many incorrect login attempts
Answer: C
Explanation:
According to IBM Spectrum Protect V8.1.9 documentation1, a security notification is displayed in the Operations Center when an SSL/TLS failure occurs2. SSL/TLS is a protocol that can secure communications between the Operations Center and the hub server, and between the hub server and associated spoke servers. If SSL/TLS fails, it might indicate a network problem or a security breach.
The other options are not valid reasons for displaying a security notification in the Operations Center. A possible ransomware attack would trigger an alert notification, not a security notification3. A restricted command does not need approval, but it is logged inthe audit log for review1. Too many incorrect login attempts would result in locking out the user account, not displaying a security notification1.

2.What is a requirement for restoring individual files from an NDMP backup with the backup/archive client GUI?
A. The FILELEVEL option must be enabled on the NAS Filer.
B. Table of Contents (TOC) must be created during the backup.
C. The NDMP API extension must be installed on the client.
D. TOCDESTINATION must be selected in front of the restore.
Answer: B
Explanation:
According to IBM documentation1, one of the requirements for restoring individual files from an NDMP backup with the backup/archive client GUI is that a Table of Contents (TOC) must be created during the backup. The TOC contains file-level restore information that is used by thebackup/archive client GUI to display and select files for restore. The TOC is stored in a different storage pool from the one where the backup image is stored.
https://www.ibm.com/docs/en/spectrum-protect/8.1.11?topic=servers-file-level-backup-restore-ndmp-operations

3.What do dissimilar policies provide in IBM Spectrum Protect node replication between source and target servers?
A. differing administrative client owners
B. differing retention of data
C. differing client node names
D. differing prioritization of client replication operations
Answer: B
Explanation:
In IBM Spectrum Protect node replication, dissimilar policies provide the ability to replicate client data between source and target servers with differing retention settings.
Dissimilar policies allow for more granular control over the retention settings of client data on the target server, which can be different from the retention settings on the source server. This means that the data

can be kept for a longer or shorter period of time on the target server compared to the source server, based on the specific retention policies configured for the target server.

According to IBM documentation1, dissimilar policies provide the ability to use different management policies on the target replication server than on the source replication server.

This means that you can have different retention periods, storage pools, or data types for replicated data on the target server. You can enable this feature by using the SET DISSIMILARPOLICIES command.

https://www.ibm.com/docs/SSEQVQ_8.1.9/srv.reference/r_cmd_dissimilarpolicies_set.html

4.Which privilege class can perform all administrative functions?

A. system

B. root

C. administrator

D. superuser

Answer: A

Explanation:

According to IBM Spectrum Protect V8.1.9 documentation1, a system administrator has the highest level of authority in IBM Spectrum Protect. A system administrator can issue any administrative command and has authority to grant or revoke privileges for other administrators.

The privilege class for a system administrator is SYstem1. The other privilege classes such as root, administrator, or superuser are not valid for IBM Spectrum Protect.

In IBM Spectrum Protect (formerly known as Tivoli Storage Manager), the system privilege class can perform all administrative functions.

The system privilege class includes the following permissions:

➾ SYSOP: System operations

➾ AUDIT: Auditing operations

➾ SECURITY: Security operations

➾ NODEADDP: Add nodes

➾ NODEDELP: Delete nodes

➾ MGMTCLAS: Management class operations

➾ DEVCLASS: Device class operations

➾ STGPOOL: Storage pool operations

➾ LIBRARY: Library operations

➾ QUERY: Query operations

➾ BACKUP: Backup and archive operations

➾ RESTORE: Restore operations

➾ ARCHIVE: Archive operations

➾ RESTOREVM: Restore virtual machine operations

➾ PROXY: Proxy operations

5.What is the move DRMEDIA command used for in Disaster Recovery Manager (DRM)?

A. to change the DRM state of a volume

B. to copy one DRM volume to another

C. to copy a DRM tape to disk

D. to change the location of the DRM database

Answer: A

Explanation:

According to IBM documentation1, the move DRMEDIA command is used for changing the DRM state of a volume. The command tracks volumes that are to be moved offsite and identifies the expired or empty volumes that are to be moved onsite.

6.What is the default client file to look in for errors in a scheduled client backup?

A. dsmerr.log

B. dsmsched.log

C. schederr.log

D. tsmerror.log

Answer: B

Explanation:

According to the IBM Spectrum Protect V8.1.9 documentation, the dsmsched.log file is the default client file that contains error logs for scheduled client backups. This file is located in the directory where the Spectrum Protect client is installed. The dsmsched.log file contains detailed information about scheduled client backups, including any error messages that may have occurred during the backup. This file is a useful tool for troubleshooting issues with client backups.
https://www.ibm.com/support/pages/collecting-data-ibm-spectrum-protect-client-backup-and-restore

7.Which process needs to be run before automatic failover can occur?

A. tier to tape

B. data deduplication

C. migration

D. node replication

Answer: D

Explanation:

In IBM Spectrum Protect, automatic failover can occur when a primary node fails and a secondary node takes over its responsibilities. In order for this to work, the secondary node must be an exact copy of the primary node. This is achieved through node replication, which synchronizes the data and configuration between the primary and secondary nodes.

Node replication is a process that needs to be set up and run before automatic failover can occur. It involves creating a copy of the primary node and configuring it as a secondary node. The data and configuration are then synchronized between the two nodes, either continuously or on a schedule.

Once node replication is set up, the secondary node can take over the primary node's responsibilities in the event of a failure, without any interruption in service.

To summarize, node replication is the process that needs to be run before automatic failover can occur in IBM Spectrum Protect.

8.Which statement is true regarding client-side and server-side deduplication?

A. Client-side deduplication only works when there is a Deduplication Cache configured on the server.

B. Client-side deduplication generally eliminates the deduplication workload on the server for that particular client workload.

C. Client-side deduplication only eliminates the deduplication workload on the server for that workload when a Deduplication Cache is configured on the client.

D. Server-side deduplication uses the Deduplication Cache to generate a hash code to be sent to the client, in order to run the client-side deduplication

Answer: B

Explanation:

According to the IBM Spectrum Protect documentation1, one statement that is true regarding client-side and server-side deduplication is B. Client-side deduplication generally eliminates the deduplication workload on the server for that particular client workload. This statement means that when client-side deduplication is enabled, the backup-archive client removes redundant data before sending it to the server, which reduces the amount of data that needs to be processed by the server.

https://www.ibm.com/docs/en/spectrum-protect/8.1.9?topic=throughput-tuning-client-side-data-deduplication

9.Which three processes can be in order to prepare for Disaster Recovery?

A. protect storage pool

B. reclamation

C. node replication

D. expiration

E. migrate node

F. backup storage pool

Answer: A,C,F

Explanation:

According to the IBM Spectrum Protect documentation1, three processes that can be used to prepare for disaster recovery are:

✑ Protect storage pool: This process creates a copy of a primary storage pool on another server or device. The copy can be used to restore data if the primary storage pool is damaged or lost.

✑ Node replication: This process replicates data from one server node to another server node. The replicated data can be used to recover client data if the source server node is unavailable.

✑ Backup storage pool: This process backs up data from a primary storage pool to another storage pool. The backup storage pool can be used to restore data if the primary storage pool is corrupted or deleted.

10.What happens by default if the journal engine service is installed and running when the incremental command is used for a backup?

A. It updates the journal database with current data after a successful backup.

B. It performs a journal-based backup on file systems that are being monitored by the journal engine service.

C. It backs up the file journal on an incremental basis.

D. It monitors the incremental backup process and collects all data that is eligible for the next journal-based full backup.

Answer: B